Finite and infinite implementation of transition systems

Hesselink, Wim H.; Renardel de Lavalette, Gerard R.

Published in:
Theoretical Computer Science

DOI:
10.1016/j.tcs.2012.08.014

Publication date:
2012

Theoretical Computer Science 458 (2012) 131–135

Contents lists available at SciVerse ScienceDirect

Theoretical Computer Science

journal homepage: www.elsevier.com/locate/tcs

Note

Finite and infinite implementation of transition systems

Wim H. Hesselink, Gerard R. Renardel de Lavalette *

Department of Computing Science, University of Groningen, P.O. Box 407, 9700 AK Groningen, The Netherlands

ARTICLE INFO

Article history:
Received 27 September 2011
Received in revised form 30 March 2012
Accepted 13 August 2012
Communicated by R. van Glabbeek

Keywords:
Transition system
Implementation
Stuttering
König's lemma
Model checking

ABSTRACT

A system T is defined as implementing a system S if every infinite execution of T leads to the same observations as some infinite execution of S. System T implements S finitely if every finite execution of T leads to the same observations as some finite execution of S. It is proved that, under certain conditions on the implemented system, finite implementation implies implementation. The proof uses König's lemma. It is shown that the conditions are essential.

1. Introduction

In the theory of computation, infinite systems are used to model finite systems, and finite systems are used to model infinite systems. For instance, even though every computer has a finite state space, infinite Turing machines are regarded as better models for them than finite state machines. On the other hand, one uses abstract interpretation to construct finite models for infinite systems. Yet the properties of infinite systems are strongly influenced by finiteness conditions imposed on them or on their constituents.

This note is devoted to one such property: the implementation relation between observable transition systems. A transition system consists of a state space X, a set A of initial states, and a set R of possible transitions between states. Executions are (finite or infinite) sequences of states, starting in an initial state and respecting the transition relation. Since we want to distinguish between externally observable and unobservable internal transitions, we extend transition systems with an observation function defined on states. Our definition of observable transition systems unifies the specifications of [1] and the Kripke structures of [2]. The paper [1] requires that transition relation R is reflexive (so it allows stuttering), and postulates a supplementary property to express liveness; the book [2] requires that the state space X is finite and the transition relation R is total. We postpone such technical decisions to the points where we need them.

The implementation relation between systems is defined by means of inclusion for the set of visible executions, as in [1]. Implementation relations are usually proved by relating the internal states of the systems, i.e. by refinement mappings or forward or backward simulations: see [1,3,6]. In this note, however, we focus on implementation and visible executions, and ignore simulation relations.

There are two ways to define implementation, using either finite or infinite executions. The main result of this note is that these two definitions are equivalent when the implementing system has a total transition relation and the implemented system allows stuttering (i.e. has a reflexive transition relation) and satisfies another property called *mildness*. Mildness imposes finiteness on certain sets of states: it holds in particular when the state space itself is finite (as is often the case in model checking). The proof of the main result uses König's lemma.

* Corresponding author. Tel.: +31 50 3637128.
E-mail address: g.r.renardel.de.lavalette@rug.nl (G.R. Renardel de Lavalette).

0304-3975/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2012.08.014

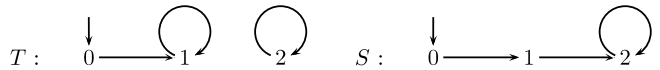

Fig. 1. Two observable transition systems T, S with total transition relations. T finitely implements S, but T does not implement S.

2. Observable transition systems and implementation

A *observable transition system* is a quadruple $S = \langle X, A, R, f\rangle$ where X is a set of states, $A \subseteq X$ is the set of initial states, $R \subseteq X^2$ is the transition relation, and $f : X \to Obs$ is the observation function (Obs is a set of observations). An *execution* of S is a (finite or infinite) nonempty sequence of states $s \in X^+ \cup X^\infty$ such that $s_0 \in A$ and $(s_i, s_{i+1}) \in R$ for all relevant indices i. We write S_+ for the set of finite executions of S and S_∞ for the set of infinite executions of S.

For later use, we introduce some notation for sequences s, t. The length of s is denoted by $\#s$, and $(s \mid n)$ denotes the prefix of s with length n (provided that $n \leq \#s$). $s \sqsubseteq t$ means that s is a prefix of t; the one-step prefix relation $s \sqsubseteq t \;\&\; \#s + 1 = \#t$ is denoted by $s \sqsubset_1 t$.

The *stuttering removal function* ρ replaces every maximal subsequence of consecutive identical elements of a sequence by a single copy of this element. (For technical reasons, we deviate slightly from the definition of the stuttering removal function $\natural$ in [1], where only *finite* maximal subsequences are replaced.) An infinite state sequence s is defined to *visibly terminate* if $\rho(f \cdot s)$ is finite (or, equivalently, if $f \cdot s$ is eventually constant). Here $f \cdot s = \langle f(s_0), f(s_1), \ldots\rangle$ denotes the application of f to the states in s. We write $S_{(\infty)}$ for the collection of visibly terminating infinite executions, so $S_{(\infty)} = \{s \in S_\infty \mid \rho(f \cdot s) \text{ is finite}\}$.

Let $f : X \to Obs$ be an observation function. We define *observational equivalence*, denoted as $\sim$, on finite and infinite observable sequences $s, t \in X^+ \cup X^\infty$ by

$$s \sim t \equiv \rho(f \cdot s) = \rho(f \cdot t).$$

It is evident that $\sim$ is an equivalence relation. In the sequel, we shall often (but not always) restrict observational equivalence to the executions of an observable transition system S, and we shall write $[s]_S$ for $\{t \in S_+ \mid t \sim s\}$, the collection of finite executions in S that are observationally equivalent to s.

Let S and T be observable transition systems. Without loss of generality, we assume that S and T have the same visibility function $f : X_S \cup X_T \to Obs$. We define *T implements S* (notation: $T \sqsubseteq S$) by

$$T \sqsubseteq S \equiv \forall t \in T_\infty \exists s \in S_\infty\ t \sim s$$

and *T finitely implements S* (notation: $T \sqsubseteq_{\mathrm{f}} S$) by

$$T \sqsubseteq_{\mathrm{f}} S \equiv \forall t \in T_+ \exists s \in S_+\ t \sim s.$$

$T \sqsubseteq S$ does not imply $T \sqsubseteq_{\mathrm{f}} S$ in general. To see this, consider e.g. the situation where $T_+ \neq \emptyset$ while $T_\infty = \emptyset$, which holds in finite systems where the transition relation has no loops: then $T \sqsubseteq S$ holds trivially while $T \sqsubseteq_{\mathrm{f}} S$ does not hold in general.

On the other hand, $T \sqsubseteq_{\mathrm{f}} S$ does not imply $T \sqsubseteq S$ either, as is demonstrated by the example in Fig. 1. T and S both have the state space $\{0, 1, 2\}$, the set of initial states $\{0\}$, and the identity as observation function; the transition relations are $R_T = \{(0, 1), (1, 1), (2, 2)\}$ and $R_S = \{(0, 1), (1, 2), (2, 2)\}$. Observe that both relations R_T and R_S are total but not reflexive. System T finitely implements S, but the (unique) infinite execution $\langle 0, 1, 1, 1, \ldots\rangle$ of T is not equivalent to the (unique) infinite execution $\langle 0, 1, 2, 2, 2, \ldots\rangle$ of S, so T does not implement S.

3. When are implementation and finite implementation equivalent?

We investigate conditions that imply that $T \sqsubseteq S$ and $T \sqsubseteq_{\mathrm{f}} S$ are equivalent. One direction is rather simple: we have

if $T \sqsubseteq S$ and the transition relation R_T of T is total, then $T \sqsubseteq_{\mathrm{f}} S$.

The argument runs as follows. If $t \in T_+$, then the totality of R_T implies that we can extend t to an infinite execution t' in T. Now $T \sqsubseteq S$ gives us an infinite execution s' in S with $s' \sim t'$, and this s' has a finite prefix s with $s \sim t$.

Now we look at the nontrivial direction: *under what conditions does $T \sqsubseteq_{\mathrm{f}} S$ imply $T \sqsubseteq S$?* In order to deal with the visibly terminating infinite executions in $T_{(\infty)}$, it suffices to assume reflexivity of the transition relation R_S of S. To see this, let $t' \in T_{(\infty)}$, so $t' \sim (t' \mid n + 1)$ for some n. Now $T \sqsubseteq_{\mathrm{f}} S$ gives us an execution $s \in S_+$ with $s \sim (t' \mid n + 1) \sim t'$. In order to obtain an infinite $s' \in S_\infty$ with $s' \sim t'$, it suffices to extend s to an $\sim$-equivalent infinite sequence by repeating its last element s_m infinitely often. This is possible because $(s_m, s_m) \in R_S$, which follows from the reflexivity of R_S.

So far we have dealt with straightforward results. From now on, we focus on the question: for which conditions $\mathcal{C}(S)$ on system S do we have

$$\text{if } \mathcal{C}(S) \text{ and } R_S \text{ is reflexive, then } T \sqsubseteq_{\mathrm{f}} S \text{ implies } T \sqsubseteq S\ ? \tag{1}$$

The first successful candidate for $\mathcal{C}(S)$ that we found is finiteness of the state space X_S of S. We weakened it to *finite invisibility*, i.e. the requirement that, for all observations $o \in Obs$, its inverse image $f^{-1}(o)$ in X_S is finite. This finite invisibility condition

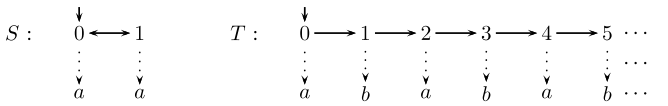

Fig. 2. Two reflexive observable transition systems S, T (the reflexive arrows are not shown). Only S has finite invisibility, and only T satisfies *fin*.

reminded us of the condition *fin* (for *finitely invisibly nondeterministic*) introduced in [1, Section 3]. Slightly simplifying, we define system S to be *fin* if

for all $s \in S_+$, the set $\rho([s]_S) = \{\rho(s') \mid s' \in S_+, s' \sim s\}$ is finite.

It turned out that (1) also holds when we take $\mathcal{C}$ to be *fin*. Yet, finite invisibility and *fin* are independent: they do not imply each other either way. This is illustrated with the systems given in Fig. 2.

System S shows that finite invisibility does not imply *fin*. It has state space $X = \{0, 1\}$, initial state 0, the constant observation function f with $f(0) = f(1) = a$ and the transition relation $R = X^2$. S has finite invisibility, because its state space is finite. However, it is not *fin*: the finite execution $s = \langle 0\rangle$ has an infinite set $\rho([s]_S)$, which corresponds to the regular expression $(01)^*0 \mid (01)^+$.

System T shows that condition *fin* does not imply finite invisibility. It has state space $\mathbb{N}$, initial state 0, the observation function $f : \mathbb{N} \to \{a, b\}$ with $f(x) = a$ iff x is even, and the transition relation $R = \{(x, y) \mid y = x \vee y = x + 1\}$. The only executions are stuttering prefixes of the infinite sequence $\langle 0, 1, 2, \dots\rangle$. For every finite execution t the set $\rho([t]_T)$ has precisely one element, so T satisfies *fin*. It has no finite invisibility, because $f^{-1}(a)$ and $f^{-1}(b)$ are infinite.

The incomparability of finite visibility and *fin* suggested looking for a common weakening. We found such a property and called it mildness. Before we present its definition, we introduce some relevant notions.

Let $S = \langle X, A, R, f\rangle$ be an observable system. States $x, y \in X$ are *observably equivalent* whenever $f(x) = f(y)$, and $E_f = \{(x, y) \in X^2 \mid f(x) = f(y)\}$ is the *observable equivalence relation*. When x and y are observably equivalent and $(x, y) \in R$, then we call (x, y) a *silent step* in R. The *silent closure* of R is defined by $(R \cap E_f)^*$. In contrast to this, we call $R - E_f$ the *visible irreflexive reduction* of R. Combining these two, we obtain $\tilde{R} = (R \cap E_f)^*; (R - E_f)$, the *visible reduction* of R (here the semicolon ';' denotes relation composition). This notion is extended to observable transition systems: $\tilde{S} = \langle X, A, \tilde{R}, f\rangle$ is the visible reduction of S.

The *reachable* part of S is defined inductively as the smallest subset $\mathsf{reach}(S)$ of X that contains A and is closed under R. One easily proves that $\mathsf{reach}(S)$ corresponds to the collection of states that occur in the executions of S.

For $x \in X$, we call $x\tilde{R} = \{y \mid x\tilde{R}y\}$ the *visible fan-out* of x.

A collection $U \subseteq X$ of states is called *quasi-observable* if $U \cap f^{-1}(o)$ is finite, for every $o \in Obs$.

Definition 1. An observable system $S = \langle X, A, R, f\rangle$ is *mild* iff A and every visible fan-out of a reachable state is quasi-observable. As a formula, this is

$$A \cap f^{-1}(o) \text{ is finite } \ \&\ \forall x \in \mathsf{reach}(S)\ (x\tilde{R} \cap f^{-1}(o) \text{ is finite}).$$

Lemma 1. *Finite invisibility implies mildness, and* fin *implies mildness.*

Proof. For finite invisibility this is evident: if $f^{-1}(o)$ is finite then so are all intersections with it. The argument for *fin* is more involved.

Assume *fin* and let $o \in Obs$. First we show that $A \cap f^{-1}(o)$ is finite. If $A \cap f^{-1}(o) = \emptyset$ we are done. So assume that $y \in A \cap f^{-1}(o)$; then $f(y) = o$ and $A \cap f^{-1}(o) = \{z \mid \langle z\rangle \in \rho([\langle y\rangle]_S)\}$, and the finiteness of $\rho[\langle y\rangle]_S$ (a consequence of *fin*) implies that $A \cap f^{-1}(o)$ is finite.

Now let $x \in \mathsf{reach}(S)$ and define $Y = x\tilde{R} \cap f^{-1}(o)$. We shall show that Y is finite. By $x \in \mathsf{reach}(S)$, we have that $x = s_n$ for some $s \in S_+$ and $n = \#s - 1$; we may assume that s is non-stuttering, i.e. $s = \rho(s)$. We claim that

$$\{s * \langle y\rangle \mid y \in Y\} \subseteq \rho([v]_S) \text{ for some } v \in S_+ :$$

from this the finiteness of Y follows, because *fin* tells us that $\rho([v]_S)$ is finite. The claim holds trivially if Y is empty, so assume that $y \in Y$. Then $f(y) = o$ and $(x, y) \in \tilde{R}$, so there is a finite sequence $t \in X^+$ with length $m + 1 > 1$ such that $t_0 = x, t_m = y$, $(t_i, t_{i+1}) \in R$ and $f(t_i) = f(x)$ for all $i < m$. As a consequence, we have that $s * \langle y\rangle \sim (s \mid n - 1) * t \in S_+$. More generally, for every $z \in Y$ we can find a sequence $u \in X^+$ with $s * \langle z\rangle \sim (s \mid n - 1) * u \in S_+$. Since $s * \langle y\rangle \sim s * \langle z\rangle$, we have that $s * \langle z\rangle \sim (s \mid n - 1) * t$ for all $z \in Y$, so we do indeed have $\{s * \langle z\rangle \mid z \in Y\} \subseteq \rho([(s \mid n - 1) * t]_S)$. This proves the claim. □

The example in Fig. 3 shows that mildness is a strict weakening of finite invisibility and of the property *fin*. We have S with state space $\mathbb{N}$, initial state 0, the observation function $f : \mathbb{N} \to \{a, b\}$ with $f(x) = a$ iff ($x = 0$ or x odd), and the transition relation $R = \{(1, 0)\} \cup \{(x, y) \mid y = x + 1\}$. It is evident that S is not finitely invisible, since both $f^{-1}(a)$ and $f^{-1}(b)$ are infinite. Neither does S satisfy *fin*, for e.g. $\rho([\langle 0\rangle]_S)$ is infinite (it corresponds with the regular expression $0(10)^*(1?)$).

On the other hand, $\tilde{R} = \{(0, 2)\} \cup \{(x, y) \mid x \neq 0 \ \&\ y = x + 1\}$, so every visible fan-out is finite, which implies that S is mild.

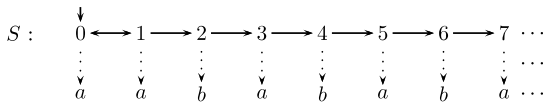

Fig. 3. A mild observable transition systems that is not finitely visible and does not satisfy *fin*.

4. The main result

In this section, we show that $T \sqsubseteq_{\mathsf{f}} S$ implies $T \sqsubseteq S$ provided that S is mild and reflexive. This comes down to: given an infinite execution t in T, find an infinite execution s of S that is observationally equivalent, i.e. with $s \sim t$. A straightforward idea is to consider the tree of all finite executions in S that are equivalent to an initial segment of s. When this tree is infinite but finitely branching, we can apply König's lemma (see [5]), which says

> every infinite, finitely branching tree has an infinite branch.

This infinite branch can then be used to obtain an infinite execution s of S. However, we cannot guarantee that $s \sim t$, because s may terminate visibly, so $s \sim (t \mid k)$ for some $k \in \mathbb{N}$. To avoid this problem, we move to the visible reduction $\tilde{S}$ of S. We shall need the following properties of $\tilde{S}$:

Lemma 2. *S and $\tilde{S}$ finitely implement each other, and $\tilde{S}$ implements S. Moreover, S is mild iff $\tilde{S}$ is mild.*

Proof. We use the mapping $\sigma : S_+ \cup S_\infty \to \tilde{S}_+ \cup \tilde{S}_\infty$, defined by

$$\begin{array}{lcl} (\sigma(s))_n & = & s_{\kappa(n)}, \text{ where} \\ \kappa(0) & = & 0 \\ \kappa(n+1) & = & \text{undefined if } \kappa(n) \text{ is undefined or if } \forall m(\kappa(n) < m < \#s \;\Rightarrow\; f(s_m) = f(s_{\kappa(n)})) \\ & = & \min\{m \mid \kappa(n) < m < \#s \;\&\; f(s_m) \neq f(s_{\kappa(n)})\} \text{ otherwise.} \end{array}$$

So $\sigma(s)$ skips states which are visibly equal to (i.e. have the same f-value as) their predecessor. As a consequence, $\rho(f \cdot s) = f \cdot \sigma(s)$ and $s \sim \sigma(s)$ for all executions s. Moreover, the restriction of σ to S_+ is surjective on $\tilde{S}_+$. To see this, consider an arbitrary execution $s \in \tilde{S}_+$. For every $i < \#s - 1$, we have $(s_i, s_{i+1}) \in \tilde{R}_S$, so there is a sequence $t(i) \in X_S^+$ that starts in s_i and ends in s_{i+1}. Now the concatenation of $t(0), \ldots t(\#s - 2)$ yields a $u \in S_+$ with $\sigma(u) = s$. Analogously, the restriction of σ to $S_\infty - S_{(\infty)}$ is surjective on $\tilde{S}_\infty$.

Now $S \sqsubseteq_{\mathsf{f}} \tilde{S}$ follows from the fact that $\sigma(s)$ is finite whenever s is finite, and $s \sim \sigma(s)$. For $\tilde{S} \sqsubseteq_{\mathsf{f}} S$ and $\tilde{S} \sqsubseteq S$, we use the surjectivity properties of σ.

S being mild iff $\tilde{S}$ is mild follows from $\tilde{\tilde{R}} = \tilde{R}$, $\mathsf{reach}(S') \subseteq \mathsf{reach}(S)$ and the fact that for every $x \in \mathsf{reach}(S)$ there is an $x' \in \mathsf{reach}(S')$ with $(x', x) \in (R_S \cap E_F)^*$ and hence $x\tilde{R}_S \subseteq x'\tilde{R}_S$. $\square$

$S \sqsubseteq \tilde{S}$ does not hold in general, due to the fact that there are no infinite executions in $\tilde{S}$ that are $\sim$-equivalent to a visibly terminating infinite execution in S. As an aside, we observe that it is possible to modify the definition of $\tilde{R}$ so that full correspondence with S is obtained. For that purpose, put $\bar{R}_S = \tilde{R}_S \cup R'$, where

$$R' = \{(x, x) \in X_S^2 \mid \exists s \in S_{(\infty)} \exists n \; (s_n = x \;\&\; (s \mid n+1) \sim s)\} \; .$$

Without proof we claim that $\bar{S} = \langle X_S, \bar{R}_S, A_S, f \rangle$ satisfies $S \sqsubseteq_{\mathsf{f}} \bar{S} \sqsubseteq_{\mathsf{f}} S$ and $S \sqsubseteq \bar{S} \sqsubseteq S$. We will not use system $\bar{S}$.

Now we can state and prove our main result.

Theorem 1. *If $T \sqsubseteq_f S$, S is mild and its transition relation is reflexive, then $T \sqsubseteq S$.*

Proof. Let S, T be given with S mild, R_S reflexive and $T \sqsubseteq_{\mathsf{f}} S$, and let t be an infinite execution of T. We have dealt with the case where t visibly terminates at the beginning of Section 3, using the reflexivity of R_S (we will not use this property of S in the rest of the present proof). So we may assume that t does not visibly terminate. We shall construct an infinite execution s of $\tilde{S}$ with $s \sim t$. Because $t \in T_\infty - T_{(\infty)}$, we have that

$$\{\rho(f \cdot (t \mid n)) \mid n > 0\} \text{ is infinite.} \tag{2}$$

Since $T \sqsubseteq_{\mathsf{f}} S$ and $S \sqsubseteq_{\mathsf{f}} \tilde{S}$ (by Lemma 2), we have for every $n > 0$ a finite sequence $s \in \tilde{S}_+$ with $s \sim (t \mid n)$. By (2), it follows that the set

$$V = \{\langle\rangle\} \cup \{s \in \tilde{S}_+ \mid \exists n > 0 \;\; s \sim (t \mid n)\}$$

is infinite, too. Moreover, V is a collection of finite sequences that contains the empty sequence and is downward $\sqsubset_1$-closed (i.e. if $v' \sqsubset_1 v \in V$ then $v' \in V$); hence $\langle V, \sqsubset_1 \rangle$ is a tree.

We show that $\langle V, \sqsubset_1 \rangle$ is finitely branching, i.e. for every $v \in V$ the outdegree $\mathsf{deg}(v) = \#\{y \mid v * \langle y \rangle \in V\}$ is finite. First we look at the root $\langle\rangle$: here we have $\mathsf{deg}(\langle\rangle) = \#\{\langle y \rangle \mid y \in A_S \;\&\; f(y) = f(t_0)\} = \#(A_S \cap f^{-1}(f(t_0)))$, and by mildness this

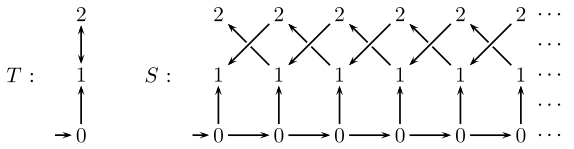

Fig. 4. Two reflexive observable transition systems S, T. The reflexive arrows are not shown, and in S only the visible second component of the states is rendered. T finitely implements S and R_S is finitely branching, but T does not implement S.

is finite. Then we consider an arbitrary nonempty $v \in V$. Let n be the maximal number with $v \sim (t \mid n)$, so $(t_{n-1}, t_n) \in R_T$ and $f(t_{n-1}) \neq f(t_n)$. Now we have (writing v_k for the final state of v)

$$\mathsf{deg}(v) = \#\{y \mid v * \langle y \rangle \in V\} \leq \#(v_k \tilde{R}_S \cap f^{-1}(f(t_n)))$$

and by mildness of $\tilde{S}$ this last set is finite.

Now König's lemma gives us an infinite branch that determines an infinite execution $s \in \tilde{S}_\infty$ with $s \sim t$. Because $\tilde{S} \sqsubseteq S$ (by Lemma 2), it follows that there is an infinite execution s' in S with $s' \sim s$; so $s' \sim t$. This ends the proof. □

4.1. Finite branching is not enough

Our initial proofs of Theorem 1 were more complicated and did not use König's lemma, although we felt that the result was related in some way. Theorem 1 becomes false, however, when the condition of mildness is replaced by the condition that the transition relation of S is finitely branching.

This is demonstrated in Fig. 4. S is the reflexive and finitely branching transition system with state space $\mathbb{N} \times \{0, 1, 2\}$, initial state $(0, 0)$, the observation function f with $f((x, y)) = y$, and the transition relation

$$\begin{aligned} R_S = {} & \{((x, y), (x, y)) \mid (x, y) \in X_S\} \\ & \cup \{((x, 0), (x + 1, 0)) \mid x \in \mathbb{N}\} \\ & \cup \{((x, 0), (x, 1)) \mid x \in \mathbb{N}\} \\ & \cup \{((x + 1, 1), (x, 2)), ((x + 1, 2), (x, 1)) \mid x \in \mathbb{N}\} \end{aligned}$$

and T is the finite and reflexive transition system with state space $\{0, 1, 2\}$, initial value 0, the identity as observation function, and transition relation R_T consisting of $(0, 0)$, $(1, 1)$, $(2, 2)$, $(0, 1)$, $(1, 2)$ and $(2, 1)$.

One easily verifies that any (finite or infinite) execution s of S starts in $(0, 0)$, proceeds to $(x, 0)$ for some $x \in \mathbb{N}$, and then possibly proceeds via $(x, 1)$, $(x - 1, 2)$, $(x - 2, 1)$, ... to an end state (modulo stutter steps) $(x - y, 1 + (y \mod 2))$. As a consequence, we have that $\rho(f \cdot s)$ is of the form $0(12)^*(1?)$, and these are exactly the observable finite executions of T. Moreover, T has an infinite execution $0(12)^\infty$ that does not correspond to any execution in S. As a consequence, T does implement S finitely, but T does not implement S.

5. Concluding remarks

The condition that system S is mild holds in particular when the state space X_S is finite. This suggests applicability to model checking. Constructors of model checkers, however, are reluctant to enforce reflexivity of the transition relation because it limits expressiveness unnecessarily. Indeed, the model checker Spin [4] even allows models with a nontotal transition relation: it calls a state without outgoing transitions an *end state*. Spin's default safety check tests for the absence of *invalid* end states. However, when verifying LTL formulas (i.e. searching for accept cycles in its Büchi automaton), Spin implicitly extends the model with stutter steps, which make its transition relation reflexive.

In the proof of the theorem, reflexivity is only needed for treating the visibly terminating executions. Indeed, the main argument in Section 4 yields that, if T implements S finitely and S is mild, every infinite execution of T that does not visibly terminate is observationally equivalent to an infinite execution of S.

The theorem itself, however, becomes invalid if we replace the assumption that R_S is reflexive by the weaker assumption that R_S is total, as witnessed by the example in Fig. 1.

In view of the relationship of condition *fin* with the soundness of prophecy variables [1] and the relationship of prophecy variables with backward simulations [6,3], it may be possible to use the theorem for a stronger soundness proof of backward simulations.

References

[1] M. Abadi, L. Lamport, The existence of refinement mappings, Theoretical Computer Science 82 (1991) 253–284.
[2] E.M. Clarke, O. Grumberg, D.A. Peled, Model Checking, MIT Press, 1999.
[3] W.H. Hesselink, Eternity variables to prove simulation of specifications, ACM Transactions on Computational Logic 6 (2005) 175–201.
[4] G.J. Holzmann, The SPIN Model Checker, Primer and Reference Manual, Addison-Wesley, 2004.
[5] D. König, Theorie der Endlichen und Unendlichen Graphen: Kombinatorische Topologie der Streckenkomplexe, Akademie-Verlag, Leipzig, 1936.
[6] N. Lynch, F. Vaandrager, Forward and backward simulations, part I: untimed systems, Information and Computation 121 (1995) 214–233.